

# Transparency in Open Government Data Portals: An Assessment of Web Tracking Practices across Europe

Stefan Stepanovic<sup>1</sup>[0000-0002-4124-6643], Leonardo Mori<sup>1</sup>[0009-0006-6305-6564], Alizée Francey<sup>1</sup>[0000-0001-8832-1332]  
and Tobias Mettler<sup>1</sup> [0000-0002-7895-7545]

<sup>1</sup> Swiss Graduate School of Public Administration, University of Lausanne, Chavannes-près-Renens, Switzerland

stefan.stepanovic@unil.ch

**Abstract:** Online web analytics and web tracking, including the use of first-party and third-party cookies, are often perceived as a "black box". Both rely on the collection of large amounts of data for various purposes - functional, analytical, and marketing - often without the user's knowledge, for legitimate purposes such as improving the user experience, as well as more controversial reasons such as targeted advertising. This issue is reinforced by Google's dominant position in web analytics, particularly through the widespread integration of Google Analytics (GA) into first-party cookies. At the same time, Europe is witnessing a rise in open government initiatives, particularly in line with the General Data Protection Regulation (GDPR), which aim to increase data transparency and accessibility for individuals. These initiatives often use open government data (OGD) portals as a means to disseminate government information. Our study, therefore, examines such platforms across Europe to determine the prevalence of web tracking activity and Google's potential involvement. Our findings reveal a nuanced use of cookies within OGD portals, characterized by a significant presence of GA cookies. This situation raises debates about privacy (especially in relation to the presence of third-party cookies), transparency, and the possibility of transitioning to more ethically responsible analytics technologies in government digital services. We propose several practical recommendations for governments to improve their privacy efforts, including removing tracking practices, adopting open source analytics solutions, conducting regular audits, and improving public awareness of web tracking practices.

**Keywords:** Web Analytics, Web Tracking, Privacy, Open Government Data, Google Analytics.

## 1 Introduction

The gradual phase-out of third-party cookies in Google Chrome, starting in 2024, marks a shift in how web analytics operate, driven by the growing focus on online privacy [1]. However, the potential impact on the public sector's expanding online presence remains unclear. This online presence is notably crucial for "open government initiatives" that leverage digital tools to enhance citizen engagement [2,3]. These initiatives, which include services such as e-citizen portals, offer innovative ways for governments to interact with the population [4].

Historically, web analytics have heavily relied on web tracking, which has been a cornerstone of the multi-billion dollar online advertising industry since the 1990s [5]. Giants like Google and Meta, which captured 56% of global digital ad revenue in 2019, have been primary beneficiaries of this model [5]. This mechanism particularly hinges on web cookies, with two key categories: first-party cookies issued by the website itself, and third-party cookies placed by external entities for cross-site tracking and data sharing [6]. In all cases, such practices support various web functionalities, including personalized content, site analytics, and social media integration [6-8]

In the European Union, the ePrivacy Directive passed in 2002 has been the first regulatory effort to inaugurate the notion of cookie consent [9] and the introduction of the General Data Protection Regulation (GDPR) in 2018 was a significant step towards enforcing strict regulations on data collection and commercial use. This regulation significantly improved the protection of users' privacy against widespread tracking by third parties, in particular through the introduction of consent requirements. However,

it is important to acknowledge that third-party cookies are still used on government websites [10]. In 2022, a study found that more than half of government websites in ten G20 countries had third-party cookies in place [11]. Even in Germany, where data protection laws are known to be strict, over 25% of government portals engaged in this practice [11].

In addition, the post-GDPR landscape reveals another paradox: while the regulation aimed to decentralize market power, it appears to have strengthened Google's dominance in various web technology segments [12]. This suggests that GDPR may inadvertently shape the market in favor of larger companies that can leverage first-party cookies data to get around eventual restrictions (such as Google, with Google Analytics) and create new standards (i.e. Google's "Privacy Sandbox", that pushes for the end of third-party cookies) [12,13]. This development therefore creates a new transition toward more opaque tracking practices, raising concerns about transparency and data stewardship online.

In light of these changes, it is important to examine open government initiatives, which are generally not expected to engage in tracking. Bounded by the GDPR, they are supposed to be guardians of good privacy practices. Additionally, they are often presented as projects that prioritize transparency, collaboration, and public participation in governance. This paper specifically concentrates on Open Government Data (OGD) portals. These portals are indeed a prominent feature of such initiatives: their core objective is to promote transparency by making government data readily available to the public [14].

The central question of our research is: "Do OGD portals track their users?" By investigating the presence of trackers, we seek to provide insight into privacy, transparency, and responsible use of tracking technologies in government services. This is especially important given the growing dominance of Google Analytics in the market. Our goal is to fully comprehend the current situation, enabling the development of policies that prioritize user interests while respecting privacy concerns. To achieve this, we utilize web scraping techniques to analyze privacy-related data from 35 countries, guided by the 2023 Open Data Maturity Scores. This group includes 27 member states of the European Union (EU), three nations of the European Free Trade Association (EFTA) (Iceland, Norway, and Switzerland), and five candidate countries for EU membership (Bosnia and Herzegovina, Montenegro, Albania, Serbia, and Ukraine).

Our study is structured as follows: first, we provide an overview of the background of the study. We then outline the research methodology and present the findings. Finally, based on these findings, we formulate recommendations and present the limitations of our work.

## 2 Background

### 2.1 About first- and third-party cookies

Individuals navigating the online sphere are subject to real-time monitoring across various websites [15,16], potentially with varying degrees of intensity [17,18]. In fact, most web services collect significant amounts of personal information from users' online activities through cookies, which constitute the core business of many online companies [6]. Cookies are small text files used to identify a computer using a network. The data stored in the cookies is generated when the computer accesses the network, and it is often labelled with a unique identifier [19]. When the computer emits a request to the website, the cookies can be sent back to the server, which allows the website to recognize the computer thanks to the identifier [19]. This web phenomenon is fueled by diverse enabling techniques [7,8]; it is ubiquitous on the internet [20] and spans across different websites and devices [21]. Beyond its role in website development and personalization [18,22], as well as advanced website analytics and integration with social networks [8,20,23], it is also commonly used for targeted advertising [8,24]. However, this information can also be used for other purposes, including price discrimination, personalization of search results, evaluating financial credibility, deciding insurance coverage, surveillance, background scanning, or identity theft [6,25-27].

Previous studies have highlighted the widespread occurrence of third-party tracking on the internet, which is a form of tracking performed by resources from other services that the one explicitly visited by

the users [23]. Hence, a first-party website authorizes a third-party website to gather users' information. Accordingly, third-party tracking enables monitoring of users' activities by services other than the one explicitly visited by the users [6,20,23,28]. This type of tracking poses a significant privacy threat, as it can collect and accumulate vast amounts of personal information (and browsing statistics) from users through many different websites [6,29]. Moreover, 80% of third-party cookies last more than a month and approximately half of those cookies remain valid for more than a year [27].

Another monitoring practice relies on first-party cookies [29]. While first-party cookies differ from third-party cookies because they aren't automatically transmitted to third parties, it is important to note that, in certain cases, tracking remains feasible [29]. This is due to the fact that any embedded third-party code that operates within the first-party website, may enable to establish or retrieve existing first-party cookies entirely and potentially disclose them to the same or different third parties [29]. While the tracking practices differ, the intrusion into user privacy remains; as tracking performed by a first party is used by a third party to circumvent standard tracking-preventing techniques [30]. However, the invasion of user privacy is even stronger in these cases (i.e., involving tracking through first-party cookies). In fact, in contrast to third-party cookies, which can be easily blocked or deleted without affecting the usability and functionality of the website, first-party cookies are not so easy to block or delete [29]. Moreover, and as noted above, while countermeasures have been implemented to address third-party cookies (e.g., browser blocking third-party cookies), these countermeasures do not target first-party cookies. This is due to the narrative that such monitoring is primarily used to enhance the user experience and improve the site through analytics [30].

More specifically, regarding analytical elements, some of the most popular cookies are Google Analytics (GA) cookies, which aim to analyze website traffic and users' behavior, including all aspects of users' journey through the website (e.g., operating systems, browser versions, session lengths, or page views) [31,32]. GA is a free web analytical tool hosted by Google that employs first-party cookies to generate detailed statistics based on users' tracking [33,34]. While GA uses a first-party cookie, set by the website's domain and visible only within that context, it also collects the users' IP as part of its operations, which may constitute individually identifiable information in specific contexts [33]. Accordingly, this raises concerns about data privacy with GA, especially given that all data resides on Google's servers [33], making GA controversial [32,35].

## 2.2 About the rationale behind OGD portals

Over the past decades, the advocacy for increased transparency has led to the advent of policy discussions, giving rise to open government initiatives [36-38]. This resulted in a democratized and technological way to enhance the accessibility of government data through OGD portals [39]. OGD portals have thus emerged as flagship open initiatives geared towards achieving a key objective: fostering transparency by disseminating government data [14]. This, in turn, aims to facilitate the accountability of governments and enable the reuse of initially disclosed data, offering social and economic value [14]. While the objective of transparency in OGD is to address information disparity, allowing citizens to observe government activities, transparency also seeks to provide a more accurate account of governments' actions [38]. The discourse on transparency has evolved beyond government actions to encompass organizations that handle diverse data types. This shift is driven by the recognition that transparency not only fosters trust but also seeks to safeguard individuals' right to privacy [40,41]. This connection between transparency and the right to privacy is the core of regulations like the GDPR, establishing standards for the transparent processing of personal data [10,42].

Considering, on the one hand, the third-party cookies and, on the other hand, the first-party cookies and the prevalence of GA in analyzing user behavior on websites, it is particularly relevant to investigate these types of trackers on OGD portals. As these portals aim to provide transparent and accessible information, understanding the types of cookies employed, including GA cookies, becomes crucial in assessing the potential impact on websites' transparency and user privacy.

### 3 Data and Methods

The data we collected are the lists of cookies used by the national OGD portals of the 35 countries included in the 2023 EU open data maturity assessment [43]. In order to obtain them, we have used the Python programming language along with Selenium, an open source project providing several tools for browser automation [44]. Selenium is a well-known tool for such web scraping, widely used in Academia (see, for example, [45] and [46]). We wrote a script that automatically (i) opens the OGD portal homepage, (ii) accepts all cookies (if the consent is requested), and (iii) after waiting for 30 seconds, collects the name and domain of all the first-party and third-party cookies used by the webpage, as well as the domains of the “frame groups”<sup>1</sup> in which the cookies are sorted. These cookies were collected on March 12th 2024<sup>2</sup>.

Once this information was retrieved, we used the cookies' domains to distinguish between first-party and third-party cookies (third-party cookies typically have a different domain associated with them). We then used the Open Cookie Database [47] - an open source initiative that categorize and describe the most commonly used cookies on the Internet -, to gather information about the function of the cookies and the controller of the data they extract. It is worth noting that all the cookies we retrieved from the OGD portals were listed in the Open Cookie Database.

### 4 Findings

Figure 1 reports the countries where the national OGD portal uses (i) third-party cookies, (ii) GA, (iii) or another web analytics solution. It also indicates (iv) where web cookies were not found during our test and, and finally (v) countries that are non-applicable. The non-applicable countries include Montenegro, whose data portal suffered a cyberattack (as indicated in the 2023 OGD maturity report) and Bosnia and Herzegovina, which is in the process of launching a national OGD portal.

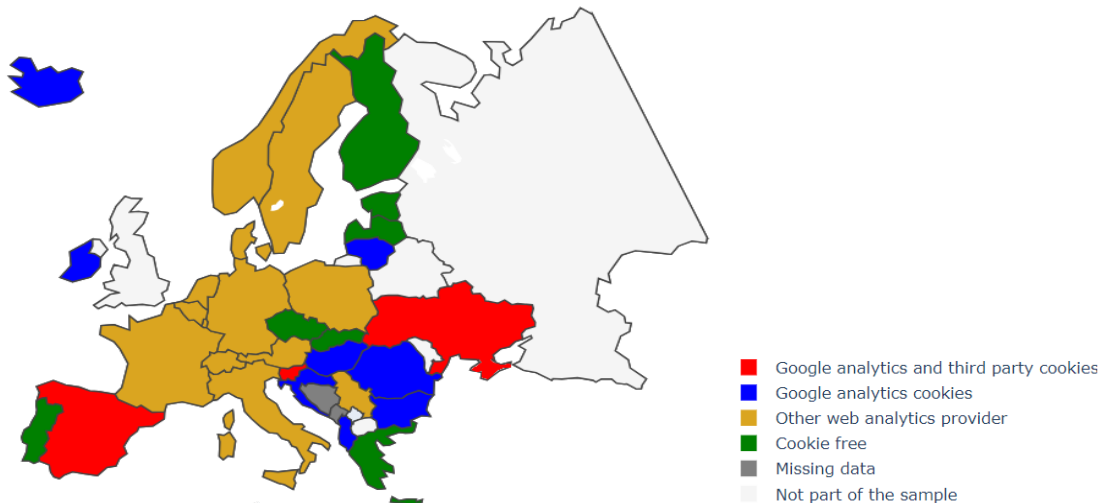


Figure 1: Map cookies usage on European OGD national platforms

We identified 12 countries that use GA (examples of recurring cookies are `_ga`, `_gid`, `_gat`). Similarly, for web analytics, we categorized 14 countries using alternative platforms: Matomo (example of recurring cookie: `_pk`; specifically in Austria, France, Germany, Italy, Luxembourg, Netherlands, Poland, Serbia,

<sup>1</sup> For an explanation about cookies and frame groups please refer to Google Chrome devtools documentation (reference in bibliography).

<sup>2</sup> The analysis of cookies on OGD portals provides a temporal snapshot that could differ due to site updates, geographical regulations, user behavior, and the browser or device utilized (e.g. system customizations or web tracking countermeasures).

Sweden, and Switzerland), SiteImprove (example of recurring cookie: *nmstat*; in Norway and Denmark), and Drupal (example of recurring cookie: *has\_js*; in Belgium and Cyprus). These platforms claim to offer fully GDPR-compliant solutions and position themselves as alternatives to GA. Nonetheless, Drupal (which is a content management system) also presents the option of incorporating a GA module.

As explained above, companies like Google and Microsoft (with cookies such as *\_clck*, *\_clsk*), offer products allowing their customers to deploy certain web functionalities, analytics or content management systems for their websites. On the other hand, platforms like Matomo and Drupal are open source, meaning that their source code is openly available and not tied to a single vendor. This openness increases transparency and auditability, while providing the ability to ensure that data remains private and secure.

In addition, three countries utilize third-party cookies, that is, domains divergent from the original OGD portal domain displayed on the site. And, ultimately, we have a relatively small proportion of OGD portals that do not have cookies (excluding the countries with missing data, seven out of 33).

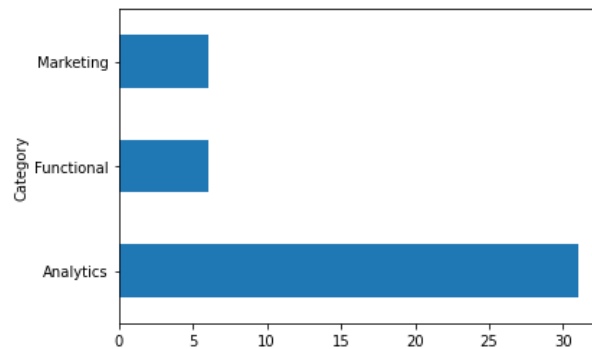


Figure 2: Cookies categories

Cookies can have different functionalities and are generally grouped in four categories depending on their purpose [47,48]. The first are functional cookies, which as the name suggests are necessary for the website to work, enabling users to navigate the site and access secure areas. The second are preference cookies, used to remember user choices, hence allowing to personalize user experience. The third are analytics cookies, which collect user behavior aggregated data in order to measure the site performance and thus enable improvements. Last come marketing cookies, that are used to deliver users relevant advertisement, based on their interests and behavior. As it will be discussed later, the distinction between analytics and marketing cookies can sometimes be blurry<sup>3</sup>. As related by Figure 2<sup>4</sup>, the majority of the cookies we collected fall under the analytics category, primarily related to GA. This is followed by the functional category, and lastly the marketing category (typically third-party cookies). It is important to note that no preference cookies were found.

## 5 Discussion

Our work aims to shed light on the black box that is web analytics, with a specific emphasis on web tracking, which may be concerning. We particularly focus on the extent of tracking activity within OGD platforms. Although OGD platforms symbolize data transparency and are central to open government initiatives, our findings first reveal the presence of third-party cookies in at least three European countries (out of 35), both within and outside the EU. This raises concerns; even if OGD platforms may not intentionally deploy third-party scripts for tracking, analytics or marketing purposes, the very existence

<sup>3</sup> For a more detailed explanation of cookies categories, please visit Cookiepedia: <https://cookiepedia.co.uk/classify-cookies>

<sup>4</sup> The counts presented in Figure 3 represent the number of different cookie types observed, not the total number of cookies. Each cookie type, regardless of its frequency across multiple sites, contributes only once to its category's tally. For instance, despite the *\_ga* cookie appearing on numerous pages, it is counted as a single entry in the analytical category.

of such scripts can be considered as problematical considering the nature of the websites. This issue persists despite the presence of consent banners, which are frequently overlooked by users (i.e. the *cookie fatigue*: the overwhelming and irritating experience of having to continuously agree to cookies on every new website visited [49,50]). In fact, there is no technical barrier preventing these third-parties, when they come from private companies, from using analytics data for tracking or profiling (and thus marketing) purposes [10].

However, it's important not solely to blame governments: the inclusion of third-party cookies in OGD platforms may not be intentional [51]. Social media links, video embeds, and "free" software modules can inadvertently introduce tracking cookies due to the business models employed by their providers [11]. Consequently, OGD platforms that rely on these external applications may inadvertently enable user tracking. Nevertheless, it is certain that the emphasis placed on transparency in the context of OGD leads individuals to not expect to encounter web tracking on OGD portals, especially in EU countries. As we have seen, this expectation is grounded in the fact that these same governments are advocating for anti-tracking measures through regulations such as the GDPR, which mandates data protection both by default and by design (Article 25). Furthermore, these platforms are funded with public money, which should not, in principle, be used to support private or commercial activities such as facilitating tracking or collecting data on citizens [10].

Zooming out, this issue largely stems from outsourcing web development for analytics purposes, coupled with the prevalence of GA in the market [52]. As mentioned, GA holds a significant market share, up to 85.8% of websites by some measures, establishing Google as the de facto standard in web analytics [13,53]. This is compounded by the dominant position of Google Chrome as a web browser, highlighting the delicate balance between utility and privacy concerns when choosing a web solution [13]. In our analysis, 11 countries (out of 35) employ GA, as revealed by the presence of well-known cookies such as `_ga`, `_gat`, and `_gid`. Yet, our intent is not to criticize these nations; rather, we highlight a grey area where their actions are not necessarily wrongful. In fact, we argue that in the larger scheme of things, giving a single corporation significant influence over data that is primarily intended to benefit citizens can be concerning. Google owns the data collected through its service, which allows it to store, use, and potentially share it [5,12,54]. This situation is therefore at odds with the data sovereignty required by European legislation. In 2019, the French data protection authority (CNIL) fined Google 50 million euros for failing to obtain valid consent [54]. Similarly, in 2022, the Austrian data protection authority found Google GA to be in violation of the GDPR [55]. These rulings also stem from the fact that websites using GA are transferring data to the United States, which, along with the potential for data to be reused without consent, is the main issue regarding data protection standards under the GDPR. Nevertheless, we have also seen that GDPR-compliant alternatives are available. This can be in the form of other private companies, such as SiteImprove (storage in the EU, does not include transfer of IP addresses to third countries). Or, it can also be, in a philosophy of transparency, open source alternatives such as Matomo [52]. These opensource alternatives offer fundamentally similar services, including data access and EU data storage, and have been adopted by some countries in our study, such as France and Italy.

Ultimately, only a few countries do not use cookies. It is not a question of better or worse: first-party cookies allow websites to remember individuals' preferences, such as the username and language, for a particular visit. This convenience eliminates the need to re-enter this information while navigating the site and can be used to collect statistics to enhance website features and user experience.

However, it's important to consider whether an OGD portal truly needs to remember all preferences. There exists a delicate balance between what is essential for improving the user experience and what may be considered superfluous.

In sum, while Google's new policy to end third-party cookies aims to enhance user privacy by reducing cross-website tracking, it raises both privacy and antitrust concerns [12]. It may still permit Google to track users through GA, potentially distorting market competition and favoring Google, leading to increased market concentration [12,13]. This situation illustrates the complex relationship between competition law and user privacy, and highlights the potential need for regulatory adjustments [13].

## 6 Implications

### 6.1 Practical implications

EU governments are primarily responsible for implementing anti-tracking measures through the GDPR, necessitating data controllers to be accountable [56]. This includes promoting open government initiatives and integrating data protection into all personal data processing activities. We argue that developers of OGD platforms and other government websites may therefore focus on the following areas:

- *Minimize unnecessary tracking:* The necessity of profiling analytics on OGD platforms is questionable. Public sector organizations, unlike private companies, have a distinct mission that does not prioritize maximizing website traffic. Instead, their primary objective should be enhancing citizen experience by ensuring easy access to required services [52]. If some analytics are deemed necessary to understand user behavior and identify improvements, a privacy-friendly, citizen-centric approach should be adopted for data collection.
- *Adopt open source products:* In line with the above point, to mitigate risks, OGD platform managers may adopt open standards and open source software. This approach reduces reliance on proprietary services and technologies and is consistent with the transparency ethos of open government initiatives [52]. Finally, a relatively simple yet radical solution is to remove (when in doubt) the highly analytical components of the code altogether [57].
- *Conduct regular audits:* Regulators in each country need to regularly conduct detailed audits to monitor third-party tracking on government websites [11,58], with the goal of quickly removing trackers. As detailed in this study, it is relatively easy for government agencies, civil society, and independent researchers to help conduct audits [58]. They can create inventories and report tracking incidents. Tools such as the Open Cookie Database [47] can also help with isolated and online checks.
- *Increase awareness about web tracking:* Data protection authorities should raise awareness about the risks of web tracking and the general loss of control over data use [59]. In fact, privacy policies on websites are often vague, broad, and lengthy, ultimately leading to the risk of uninformed online decisions [11,13,58]. For example, best practices for consent banners (although not the focus of this study) include: providing clear choices, securing consent for non-essential cookies, communicating data use transparently, documenting consent, maintaining accessibility without certain cookies, and making it easy to withdraw consent [49,50]. This means avoiding pre-checked boxes, hidden opt-out options, multiple clicks, and tracking without or prior to consent [50].

Ultimately, individuals can also protect their privacy by using browser extensions like Privacy Badger or uBlock to increase control over their personal information [60] and contribute to broader awareness and action against intrusive web tracking.

### 6.2 Theoretical implications

The theoretical implications of the study provide insights into the intersection of government transparency, web tracking, and privacy concerns. We reveal the controllers of web tracker mechanisms on OGD platforms and suggest that transparency could be enhanced by using open-source analytics software (when necessary). This also highlights the tension between privacy and utility in practice [13,53]. Organizations must balance operational efficiency and innovation with ethical considerations of privacy and data protection. This tension is further amplified by high-level regulations such as GDPR. Although the objectives and rationale of the law are clear, there are minimal procedures at a lower level (i.e. operational level) on how to implement it, as illustrated in our present study within the context of privacy and web tracking [61,62]. However, this situation also reflects the relative novelty of the regulation,

implying that practices will evolve, and increasingly evidence-based methodologies will emerge for effective compliance.

Finally, the methodological approach adopted in this study - combining web scraping techniques with an analysis of cookie functionalities/data controllers - provides a replicable design for future research in this field. This approach can be adapted and extended to other contexts, allowing scholars to conduct audits of web tracking practices across different sectors and regions.

## 7 Limitations and Concluding Remarks

Our study has primarily examined cookies as a component of online tracking. However, beyond the scope of first-party and third-party cookies, a variety of techniques are employed to monitor and analyze online user behavior. These techniques leverage different features of web technologies for tracking purposes. Key methods include, for instance, web beacons and fingerprinting [51,63]. Web beacons are invisible images or small code snippets embedded in websites and emails, enabling the tracking of user activities (i.e. website visits). This is achieved by making a request to a server for the image, which logs this request [63]. Fingerprinting collects data on a user's device and browser configurations[64], such as screen resolution, operating system, and font types, to generate a unique identifier for the device [65]. Fingerprinting can track users across different browsing sessions, even in private mode, as it does not depend on cookies [64]. Thus, our findings likely underrepresent the full extent of web tracking's pervasiveness, which concretely highlights a need for further investigation.

An additional limitation of our research is that we did not focus on analyzing cookie consent mechanisms, which are closely related to GDPR requirements for privacy management and online personal data protection. This includes the variability and complexity that users encounter when managing their preferences, especially when opting out (which is a major concern under the GDPR [51]). Such variability in user interface design for cookie management may indeed alter the opt-out process by making it complex and discouraging [50,51]. And, as we have outlined, this can lead to "cookie fatigue", i.e., the annoyance experienced by users due to the frequent requests for cookie permissions on websites [66].

Due to the format of the study, we also did not perform an in-depth content analysis of the cookies. Examining the content of these cookies could reveal whether they store information that could potentially be used for tracking, such as unique identifiers. We recommend that future research include this analysis to provide a more detailed understanding of the tracking capabilities of specific cookies.

In conclusion, our findings reveal a relatively widespread use of ready-made analytical solutions, first among all GA. Even though such products certainly provide good quality services and have somehow become a standard practice in web development, we believe that it is important for governments to consider the consequences of using these analytical suites. Indeed, using such products can allow foreign big tech companies to gain access to European citizens online behavior data, and to stock it outside Europe, which does not align with the GDPR [54,55]. Additionally, besides legal considerations, it is often impossible to clearly rule out the possibility that data collected with analytical cookies will not be used for marketing purposes [13,35]. Therefore, it is essential for governments to align their practices in developing OGD portals with the privacy recommendations they issue. This ensures coherence and transparency, which are the leading motivations behind OGD initiatives [14]. Although digitalization is often viewed as a means of improving the efficiency of public administration, it should not lose sight of its primary goal of enhancing the quality of public services and making them accessible and fair to all citizens.

**Acknowledgments.** This study was funded by the Swiss National Science Foundation (grant number 212637). We would like to give a special thanks to Hugo Hueber, research engineer at the University of Lausanne, for his support.

**Disclosure of Interests.** The authors have no competing interests to declare that are relevant to the content of this article.



## References

1. Cooper, D.A., Yalcin, T., Nistor, C., Macrini, M., Pehlivan, E.: Privacy considerations for online advertising: A stakeholder's perspective to programmatic advertising, *Journal of Consumer Marketing* 40 (2), pp. 235-247, (2023)
2. Soguel, N., Bundi, P., Mettler, T., Weerts, S.: *Comprendre et concevoir l'administration publique.*, 1st edition ed., EPFL Press(2023)
3. Wirtz, B.W., Weyerer, J.C., Becker, M., Müller, W.M.: Open government data: A systematic literature review of empirical research, *Electronic Markets* 32 (4), pp. 2381-2404, (2022)
4. Schedler, K., Guenduez, A.A., Frischknecht, R.: How smart can government be? Exploring barriers to the adoption of smart government, *Information Polity* 24 (1), pp. 3-20, (2019)
5. Johnson, G.: Economic research on privacy regulation: Lessons from the GDPR and beyond, (2022)
6. Bujlow, T., Carela-Español, V., Solé-Pareta, J., Barlet-Ros, P.: A Survey on Web Tracking: Mechanisms, Implications, and Defenses, 105 (8), pp. 1-34, (2017)
7. Besson, F., Bielova, N., Jensen, T., Hybrid Information Flow Monitoring Against Web Tracking, 26th Computer Security Foundations Symposium, pp. 240-254. IEEE, New Orleans, USA (2014)
8. Sanchez-Rola, I., Ugarte-Pedrerp, X., Santos, I., Bringas, P.G.: The Web is Watching You: A Comprehensive Review of Web-Tracking Techniques and Countermeasures, *Logic Journal of the IGPL* 25 (1), pp. 18-29, (2016)
9. Debusseré, F.: The EU e-privacy directive: a monstrous attempt to starve the cookie monster?, *International journal of law and information technology* 13 (1), pp. 70-97, (2005)
10. Samarasinghe, N., Adhikari, A., Mannan, M., Youssef, A., Et Tu, Brute? Privacy Analysis of Government Websites and Mobile Apps, ACM Web Conference, ACM, Lyon, France, 2022, pp. 564-575.
11. Gotze, M., Matic, S., Iordanou, C., Smaragdakis, G., Laoutaris, N., Measuring web cookies in governmental websites, Proceedings of the 14th ACM Web Science Conference 2022, Barcelona, Spain, 2022, pp. 44-54.
12. Peukert, C., Bechtold, S., Batikas, M., Kretschmer, T.: Regulatory spillovers and data governance: Evidence from the GDPR, *Marketing Science* 41 (4), pp. 746-768, (2022)
13. Geradin, D., Katsifis, D., Karanikioti, T.: Google as a de facto privacy regulator: Analyzing Chrome's removal of third-party cookies from an antitrust perspective, (2020)
14. Lourenço, R.P.: An Analysis of Open Government Portals: A Perspective of Transparency for Accountability, *Government Information Quarterly* 32 (3), pp. 323-332, (2015)
15. Gomer, R., Rodrigues, E.M., Milic-Frayling, N., Schraefel, M.C., Network Analysis of Third Party Tracking: User Exposure to Tracking Cookies Through Search, In: IEEE/WIC/ACM (ed.) International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT), vol.°1, pp. 549-556. IEEE, Atlanta, USA (2013)
16. Falahrastegar, M., Haddadi, H., Uhlig, S., Mortier, R., Tracking Personal Identifiers Across the Web, International Conference on Passive and Active Network Measurement, pp. 30-41. LNCS, Springer, Heraklion, Greece (2016)
17. Ermakova, T., Hohensee, A., Orlamünde, I., Fabian, B.: Privacy-Invasive Mechanisms in E-Commerce - A Case Study on German Tourism Websites, *International Journal of Networking and Virtual Organisations* 20 (2), pp. 105-126, (2017)
18. Ermakova, T., Fabian, B., Bender, B., Klimek, K., Web Tracking – A Literature Review on the State of Research, 51st Hawaii International Conference on System Sciences, Hilton Waikoloa Village, Hawaii, 2018, pp. 4732-4741.
19. What are Cookies?, <https://www.kaspersky.com/resource-center/definitions/cookies>, last accessed May 2024
20. Roesner, F., Kohna, T., Wetherall, D., Detecting and Defending Against Third-Party Tracking on the Web, 10th International Conference on Web and Social Media, pp. 155-168. San Jose, USA (2012)
21. Brookman, J., Rouge, P., Alva, A., Yeung, C., Cross-Device Tracking: Measurement and Disclosure, *Privacy Enhance Technologies*, 2017, pp. 133-148.
22. Fourie, I., Bothma, T., Information Seeking: An Overview of Web Tracking and the Criteria for Tracking Software, in: Aslib (Ed.) 2007, pp. 264-284.
23. Mayer, J.R., Mitchell, J.C., Third-Party Web Tracking: Policy and Technology, IEEE symposium on security and privacy, pp. 413-427. IEEE, San Francisco, CA (2012)
24. Parra-Arnau, J.: Pay-Per Tracking: A Collaborative Masking Model for Web Browsing, *Information Sciences* 1 (385), pp. 96-124, (2017)

25. Mikians, J., Gyarmati, L., Erramilli, V., Laoutaris, N., Detecting Price and Search Discrimination on the Internet, 11th ACM Workshop on Hot Topics in Network, ACM, Washington, USA, 2012, pp. 79-84.
26. Hannak, A., Soeller, G., Lazer, D., Mislove, A., Wilson, C., Measuring Price Discrimination and Steering on E-Commerce Web Sites, Internet Measurement Confer, ACM, Vancouver, BC, Canada, 2014, pp. 305-318.
27. Samarasinghe, N., Mannan, M.: Towards a Global Perspective on Web Tracking, *Computers & Security* 87 (101569), pp. 1-13, (2019)
28. Li, T.-C., Hang, H., Faloutsos, M., Efstathopoulos, P., TrackAdvisor: Taking Back Browsing Privacy from Third-Party Trackers, 16th Passive and Active Measurement Conference, Springer International Publishing, New York, USA, 2015, pp. 1-12.
29. Chen, Q., Ilija, P., Polychronakis, M., Kapravelos, A., Cookie Swap Party: Abusing First-Party Cookies for Web Tracking, 2021 ACM Web Conference, Ljubljana, Slovenia, 2021, pp. 2117-2129.
30. Demir, N., Theis, D., Urban, Z., Pohlmann, N.: Towards Understanding First-Party Cookie Tracking in the Field, arXiv preprint arXiv:2202 (01498), pp. 1-20, (2022)
31. Pantelic, O., Jovic, K., Krstovic, S.: Cookies Implementation Analysis and the Impact on User Privacy Regarding GDPR and CCPA Regulations, *Sustainability* 14 (9), pp. 1-14, (2022)
32. The End of Google Analytics in Europe?, <https://www.activemind.legal/guides/google-analytics/>, last accessed 2024/12. January
33. Loftus, W.: Demonstrating Success: Web Analytics and Continuous Improvement, *Journal of Web Librarianship* 6 (1), pp. 45-55, (2012)
34. Plaza, B., Monitoring Web Traffic Source Effectiveness with Google Analytics: An Experiment with Time Series, Aslib, Emerald Group Publishing Limited, 2009, pp. 474-482.
35. Is Google Analytics 4 GDPR-compliant?, <https://usercentrics.com/knowledge-hub/google-analytics-and-gdpr-compliance-rulings/#:~:text=Under%20the%20GDPR%2C%20companies%20using,significant%20fines%20and%20legal%20repercussions>, last accessed 2024/12. January
36. Bertot, J.C., Jaeger, P.T., Grimes, J.M.: Using ICTs to Create a Culture of Transparency: E-Government and Social media as Openness and Anti-Corruption Tools for Societies, *Government Information Quarterly* 27 (3), pp. 264-271, (2010)
37. McDermott, P.: Building Open Government, *Government Information Quarterly* 27 (4), pp. 401-413, (2010)
38. Matheus, R., Janssen, M.: A Systematic Literature Study to Unravel Transparency Enabled by Open Government Data: The Window Theory, *Performance & Management Review* 43 (3), pp. 503-534, (2020)
39. Open Government Data - What is Open Government Data?, <https://www.oecd.org/gov/digital-government/open-government-data.htm>, last accessed 2022/14. March
40. Nougères, A.B., Privacy is Key in Processing Personal Data by AI: UN Expert, United Nations, Online, 2023.
41. Tolbert, C.J., Mossberger, K.: The Effects of E-Government on Trust and Confidence in Government, *Public Administration Review* 66 (3), pp. 354-369, (2006)
42. Official Journal of the European Union, Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016, pp. 1-88.
43. data.europe.eu, 2023 Open Data Maturity Report, 2023, p. 152.
44. Selenium documentation, <https://www.selenium.dev/>, last accessed 2024/03/12
45. Rasaii, A., Singh, S., Gosain, D., Gasser, O., Exploring the cookieverse: A multi-perspective analysis of web cookies, International Conference on Passive and Active Network Measurement, Springer, 2023, pp. 623-651.
46. Englehardt, S., et al., Cookies that give you away: The surveillance implications of web tracking, Proceedings of the 24th International Conference on World Wide Web, Florence, Italy, 2015, pp. 289-299.
47. Open Cookie Database, <https://github.com/jkwakman/Open-Cookie-Database?tab=readme-ov-file>, last accessed 2024/03/12
48. Kretschmer, M., Pennekamp, J., Wehrle, K.: Cookie banners and privacy policies: Measuring the impact of the GDPR on the web, *ACM Transactions on the Web (TWEB)* 15 (4), pp. 1-42, (2021)
49. Pantelic, O., Jovic, K., Krstovic, S.: Cookies implementation analysis and the impact on user privacy regarding GDPR and CCPA regulations, *Sustainability* 14 (9), p. 5015, (2022)

50. Habib, H., Li, M., Young, E., Cranor, L., "Okay, whatever": An evaluation of cookie consent interfaces, Proceedings of the 2022 CHI conference on human factors in computing systems, 2022, pp. 1-27.
51. Papadogiannakis, E., Papadopoulos, P., Kourtellis, N., Markatos, E.P., User tracking in the post-cookie era: How websites bypass gdpr consent to track users, Proceedings of the web conference 2021, 2021, pp. 2130-2141.
52. Gamalielsson, J., et al.: Towards open government through open source software for web analytics: The case of Matomo, JeDEM-eJournal of eDemocracy and Open Government 13 (2), pp. 133-153, (2021)
53. Alby, T., Popular, but hardly used: Has Google Analytics been to the detriment of Web Analytics?, Proceedings of the 15th ACM Web Science Conference 2023, 2023, pp. 304-311.
54. Urban, T., Tatang, D., Degeling, M., Holz, T., Pohlmann, N., Measuring the impact of the GDPR on data sharing in ad networks, Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, 2020, pp. 222-235.
55. Winklbauer, S., Horner, R.: Austrian DPA Decides EU-US Data Transfer through the use of Google Analytics to Be Unlawful, Eur. Data Prot. L. Rev. 8, p. 78, (2022)
56. Kollnig, K., Shuba, A., Van Kleek, M., Binns, R., Shadbolt, N., Goodbye tracking? Impact of iOS app tracking transparency and privacy labels, Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency, Seoul, South Korea, 2022, pp. 508-520.
57. Tahaei, M., Li, T., Vaniea, K.: Understanding Privacy-Related Advice on Stack Overflow, Privacy Enhancing Technology 2022 (2), pp. 114-131, (2022)
58. Libert, T., An automated approach to auditing disclosure of third-party data collection in website privacy policies, Proceedings of the 2018 World Wide Web Conference, 2018, pp. 207-216.
59. The Federal Council, Federal Data Protection and Information Commissionner, <https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/grundlagen.html>, last accessed January 2024
60. Borgolte, K., Feamster, N., Understanding the performance costs and benefits of privacy-focused browser extensions, Proceedings of The Web Conference 2020, Taipei, Taiwan, 2020, pp. 2275-2286.
61. Várkonyi, G.G., Gradišek, A.: Data protection impact assessment case study for a research project using artificial intelligence on patient data, Informatica 44 (4), pp. 1-10, (2020)
62. Karami, F., Basin, D., Johnsen, E.B., DPL: A Language for GDPR Enforcement, 2022 IEEE 35th Computer Security Foundations Symposium (CSF), IEEE, Haifa, Israel, 2022, pp. 112-129.
63. Kashi, E., Zavou, A., Did I Agree to This? Silent Tracking Through Beacons, HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22, Springer, 2020, pp. 427-444.
64. Al-Fannah, N.M., Mitchell, C.: Too little too late: can we control browser fingerprinting?, Journal of Intellectual Capital 21 (2), pp. 165-180, (2020)
65. Acar, G., et al., The web never forgets: Persistent tracking mechanisms in the wild, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, USA, 2014, pp. 674-689.
66. Bollinger, D., Kubicek, K., Cotrini, C., Basin, D., Automating cookie consent and {GDPR} violation detection, 31st USENIX Security Symposium (USENIX Security 22), Boston, USA, 2022, pp. 2893-2910.